IBM Security

Security trends in the retail industry

Cybercrime focus shifts to online retailers and smaller businesses

IBM X-Force® Research
Managed Security Services Report

IBM

Click here to start ▶

Contents

Executive overview

This paper starts with a review of the most prevalent attacks targeting the retail industry, with a deep dive into a specific kind of attack: malware and how it's infecting point of sale systems. Next we turn from discussing traditional network cybersecurity to reviewing trends in retail fraud, focusing on how the threat model is changing with the advent of mandated integrated chip (IC) card use in the US. We wrap up with a series of recommendations for protecting against prevalent cybersecurity attacks and helping reduce fraud.

Our recent IBM report, *The price of loyalty programs*, examined cybersecurity risks to customer rewards programs in the retail, air travel, hotel, and financial services industries.[1] Unfortunately, those threats aren't the retail industry's only security concern; brute force attacks on loyalty account passwords are just one part of an alarming picture. In 2014, according to the *IBM 2015 Cyber Security Intelligence Index*, retailers and wholesalers experienced fully 50 percent more security incidents than in 2013.

Since then, we've seen several trends. Attacks involving malware are high, making up most of the threat activity observed across IBM® Managed Security Services client networks, and malware is the leading attack type in breaches according to IBM X-Force® Interactive Security Incidents data. While proven attack vectors such as Shellshock and SQL injection continue to plague retailers, accounting for nearly 28 percent of attack activity, an interesting trend we'll be following in 2016 is the use of the Tor network to target the industry.

The financial damage is escalating. As the *2015 Cost of Data Breach Study: Global Analysis* reports, "while the cost of data breach stayed relatively constant for most industries, the retail sector experienced a significant increase, from $105 [per record] in 2014 to $165 in 2015."[2] Given the sheer volume of breaches—almost 236 million records are known to have been compromised since 2011[3]—that means losses in the billions.

Retailers are most likely to experience attacks involving malware, with losses in the billions of dollars.

Contents

We're seeing a shift in attackers' focus. With security controls tightened in large businesses, attackers are going after smaller businesses. The payoff per target may be lower, but the targets are easier and far more numerous. Analysts are finding it difficult to assess the true impact of this shift because many smaller retailers aren't reporting the number of compromised records in their disclosures.

With the shopping season now in full swing, we also assessed attack data from the Black Friday/Cyber Monday weekend. Those days might seem a good time for increased attacks, but historically we haven't seen a sharp uptick. This year fared no differently, with the daily average number of attacks only slightly above the daily average for the year.

About this report

This IBM X-Force Research report was created by the IBM Managed Security Services Threat Research group, a team of experienced and skilled security analysts working diligently to keep IBM clients informed and prepared for the latest cybersecurity threats. This research team analyzes security data from many internal and external sources, including event data, activity and trends sourced from the tens of thousands of endpoints managed and monitored by IBM.

Contents

In addition, for 2015 some have raised concern that this year's switch to chip cards for in-store purchases in the United States would shift the majority of fraudulent transaction attempts to online stores, and it appears that this might indeed be the case. For example, a third-party study found that fraud rates for transactions that don't involve physically swiping a card have increased in 2015, with 1 in 86 transactions a fraudulent attempt compared to 1 in every 114 in 2014.[4]

This leads us to comment on the chip-and-PIN card versus chip-and-signature cards discussion, which peaked this year with the deadline for merchants and card issuers in the United States to be EMV-compliant by October 1, 2015. EuroPay, MasterCard, and Visa (EMV) cards, also called smart cards, chip cards, or IC cards, store their data on integrated circuits rather than magnetic stripes, although many also have stripes for backward compatibility. The shift of credit card fraud liability from card issuers to merchants that are not compliant has already happened in many parts of the world.[5] While the debate over which type of card is more secure may be important, we wonder how relevant it really is, given that cards themselves will most likely become things of the past in the not too distant future.

With all the concerns plaguing the retail industry, organizations need to understand the trends and make the security investments that best respond to them. Our recommendations are meant to optimize security programs to stop advanced threats and protect the "crown jewels."

With chip cards providing higher fraud protection for in-store purchases, fraudulent transaction attempts are shifting to online stores.

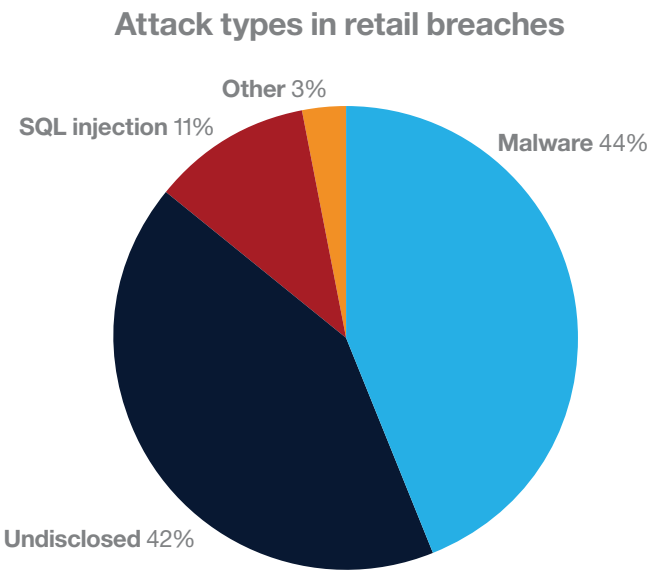
Contents

Prevalent attacks targeting the retail industry

IBM Managed Security Services continuously monitors billions of events reported every year by more than 8,000 client devices in over 100 countries. Analysis of the data accumulated between January 1, 2015, and November 30, 2015, reveals some interesting findings about attacks against the retail industry.

Malicious documents and sites

As in most other industries, attacks aimed at fooling victims into opening malicious documents or clicking on links to malicious sites are proving very successful in retail. The intent is almost always to have the victim download malware. These attacks, more than half of them exploiting file image and media player vulnerabilities, accounted for nearly 18 percent of the total attacks observed. It should come as no surprise that 44 percent of all the retail breaches disclosed since 2011 were due to malware (see Figure 1).



Source: IBM X-Force Interactive Security Incidents data (January 1, 2011 – November 30, 2015).[9]

Figure 1. "Malware" ranked first as most prevalent attack type affecting the retail industry.
Note: Data is a sampling of notable incidents for each year and not a full representation of all incidents.

Contents

SQL Injection

A tried and true attack vector, SQL injection accounts for 14 percent of attacks. Although it's been around since 1995, it's still one of the most common attacks on web assets. Weak SQL database security policy is a common denominator in successful attacks. SQL injection is also the number two attack type associated with retail security breaches (see Figure 1). It's also the attack method used in the second largest breach reported this year.[6] SQL injection attacks have been responsible for the compromise of over 112 million records across all industries since 2011.[7]

Shellshock

Shellshock is the new SQL Slammer, a computer worm that first surfaced in January 2003. One of the threat game changers for 2014, Shellshock is the number three attack vector, accounting for over 13 percent of attacks in the retail industry. Shellshock is a vulnerability in the GNU Bash shell widely used on Linux, Solaris and Mac OS systems and is well documented by the IBM *2015 Cyber Security Intelligence Index*. Like SQL Slammer, Shellshock has staying power because it's relatively simple to exploit and the exploitations are very effective. Organizations need to ensure they apply appropriate patches to address the vulnerability.

Honorable Mention: Attacks from the Tor network

This year there's been a lot of talk about Tor. As described in the IBM paper *Dangers of the deep, dark web*, criminals often use the Tor network to hide or communicate and trade with each other without exposing the content of their transactions, and as a launch pad for attacks against surface web targets.[8] Five percent of attacks targeting the retail industry came from the Tor network—a percentage that may not appear significant until you realize that it is a higher percentage than other industries experience.

Contents

A rain of malware in security incidents

Analyses by IBM Managed Security Services and IBM X-Force Interactive Security Incident breach data agree on the most prevalent attack types targeting the retail industry. Attacks involving malicious documents and links are the number one attack seen across the threat landscape, with the intent almost always to have the victim download malware.

POS vendors: One malware, endless compromises

Sometimes it takes just one attack vector affecting a popular application to cause an endless amount of damage. Take for example an exploit circulating the Internet that targets a vulnerability in a popular content management system. That single exploit has the potential to be used against thousands of sites. The same pattern holds true for a vulnerability in point of sale (POS) software.

Malware of any variety is bad enough, but retail and a few other industries have the added concern of addressing POS malware, which is designed to extract customer payment card data and send it back to a command and control server controlled by the attackers. Half of the ten largest retail breaches recorded since 2011 were caused by POS malware. These compromises resulted in the theft of nearly 195 million records, the majority containing credit card data.[10]

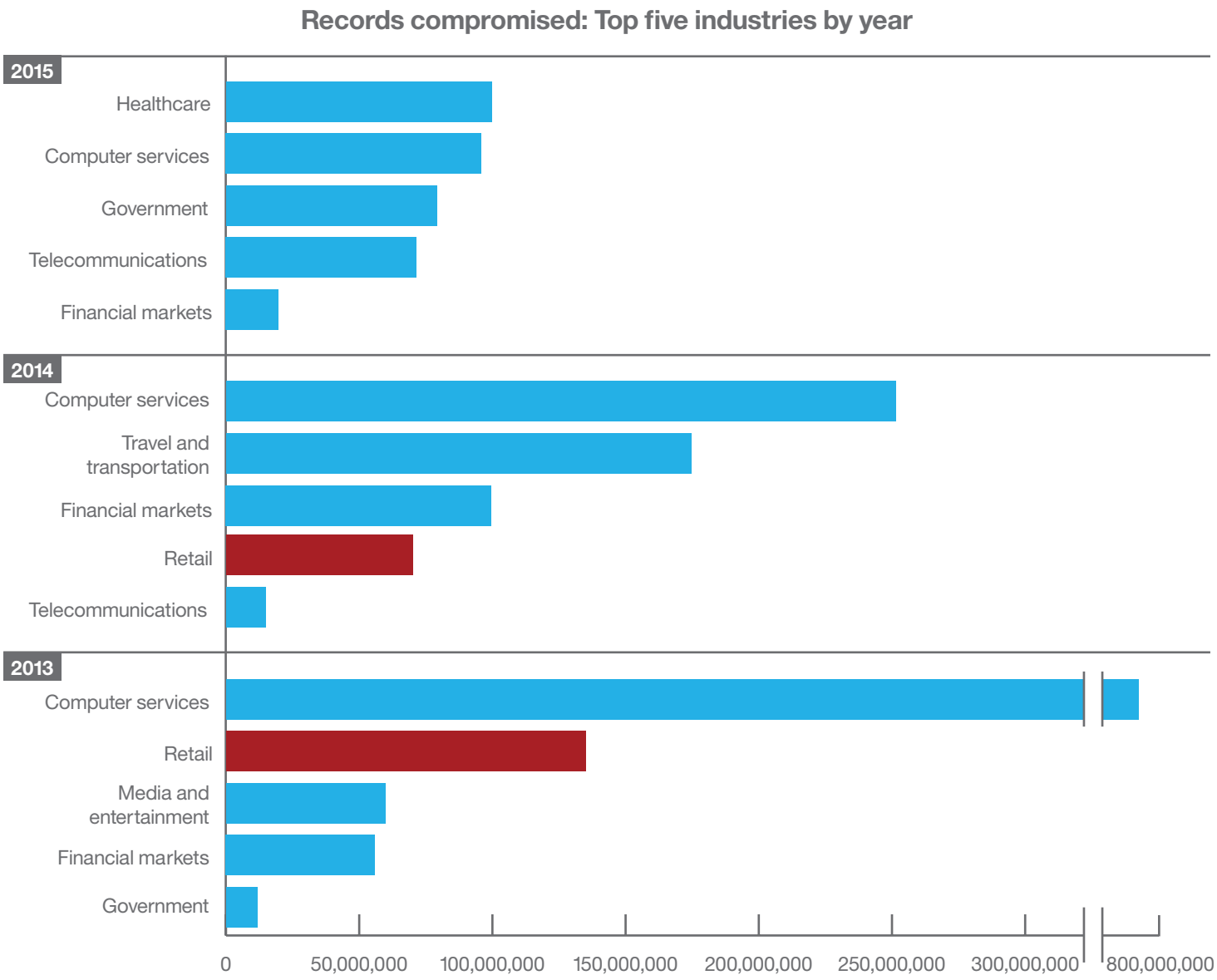
Even malware that's not considered primarily POS malware can harm the retail industry. For instance, the banking Trojan dubbed "Shifu" by IBM X-Force has an interest beyond defrauding bank accounts.[11] It scans infected endpoints for strings that may indicate it has landed on a POS endpoint and, when it finds one, it deploys a RAM-scraping plugin to siphon payment card data.

Aside from POS malware, retailers are also vulnerable to the everyday variety. Recently IBM Security Trusteer® analysts noticed the insidious Dyre malware adding new retail targets to its configuration file, preying on online customer orders, most probably to take advantage of the holiday shopping season. Earlier this year IBM Security identified an active campaign using a variant of Dyre malware that successfully stole more than $1 million from targeted organizations.[12]

Breaches occurring, numbers not being reported

The retail industry has ranked among the top five industries in terms of records compromised from a security incident from 2012 through 2014 (Figure 2), but it's been falling in rank since 2013. As of the end of November 2015 it had dropped out of the top five.

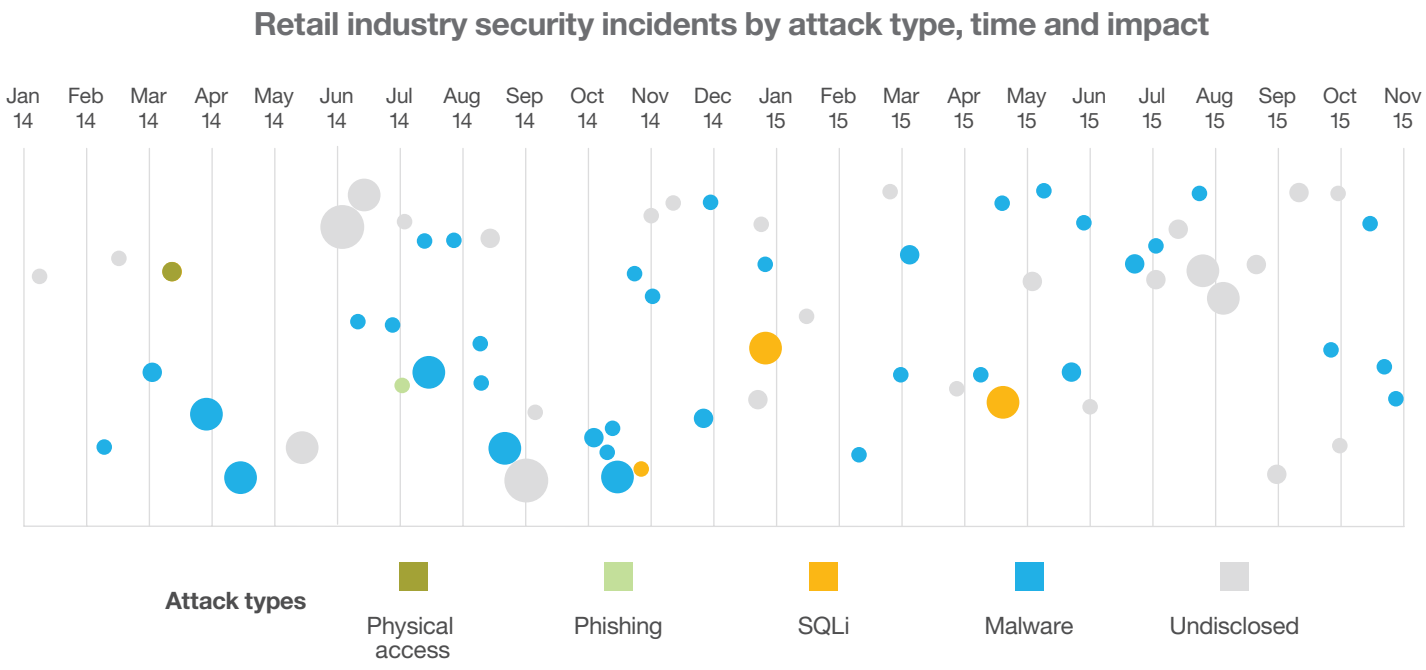
Contents



Source: IBM X-Force Interactive Security Incidents data (January 1, 2013 – November 30, 2015).[13]

Figure 2. Top 5 industries in terms of total records compromised.
Note: Data is a sampling of notable incidents and not a full representation of all incidents.

Contents



Size of circle estimates relative impact of incident in terms of cost to business.

Source: IBM X-Force Interactive Security Incidents data (January 1, 2014 – November 30, 2015).[14]

Figure 3. Retail security incident timeline.
Note: Data is a sampling of notable incidents and not a full representation of all incidents. Conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses.

While the number of compromised retail records reported is down significantly in 2015, the number of retail security incidents reported as of November 30, 2015, has already surpassed 2012 and 2013 fiscal year end disclosures. That apparent contradiction—more incidents reported but fewer records compromised—might be explained by the percentage of 2015 incidents reported in which the number of records compromised was not disclosed. As of November 30, that figure stood at a staggering 70 percent, much higher than in previous years.

Contents

Attackers shifting their focus to smaller businesses

We're seeing a small tactical shift among attackers, from targeting a few large organizations to targeting a larger number of smaller businesses. One theory behind this shift is that a lot of little payoffs will add up the same as a few big ones. Then too, large breaches can often be less effective because the compromised credit cards get shut down much faster than if a smaller business is targeted. In a large compromise, the retailer provides all the affected credit card numbers to the bank, which deactivates them immediately, but when a small company is targeted, those cards might stay active until they're caught individually, one by one. Smaller companies may also lack the resources to discover the compromise, allowing attackers to reap the benefits for a long time.

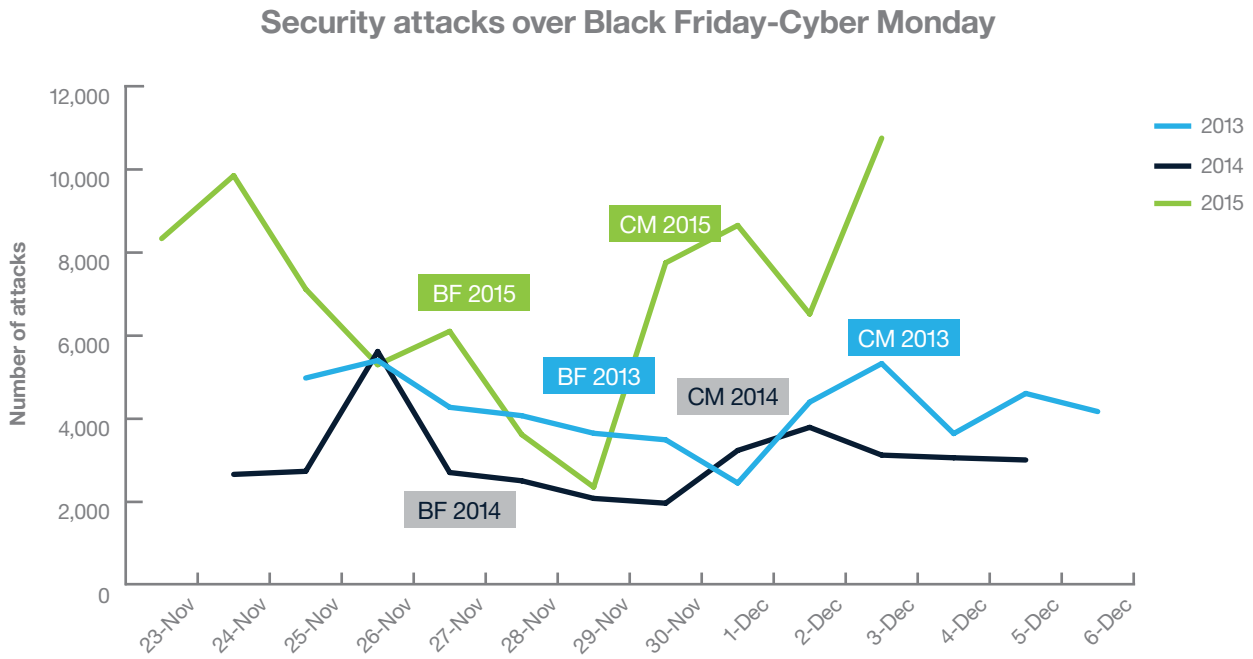
Compromises of large businesses are still happening despite the trend towards smaller targets. One of the most significant breaches this year affected a large UK-based mobile phone vendor. A sophisticated attack targeting several of the company's e-commerce website brands may have resulted in the theft of encrypted credit card numbers and other sensitive customer data affecting 2.4 million records.[15]

Smaller companies with less sophisticated defenses are attractive targets for cyber criminals.

Attackers are shopping, not attacking

Attackers use the holiday season to their advantage via spam, phishing and compromised websites, and we certainly see an increase in malicious holiday-themed activity at this time of year. Surprisingly, though, IBM security research shows that on average there is not a significant uptick in activity across all industries, including retail, during the Black Friday/Cyber Monday period (see Figure 4). In fact, the 2015 daily average alert count for the Black Friday through Cyber Monday timeframe is only slightly higher than the daily average for the year.

The threat landscape also remains relatively unremarkable when focusing specifically on the retail industry (see Figure 5). While the traffic may appear to spike on Cyber Monday this year, it is only slightly above average for the Black Friday through Cyber Monday timeframe.



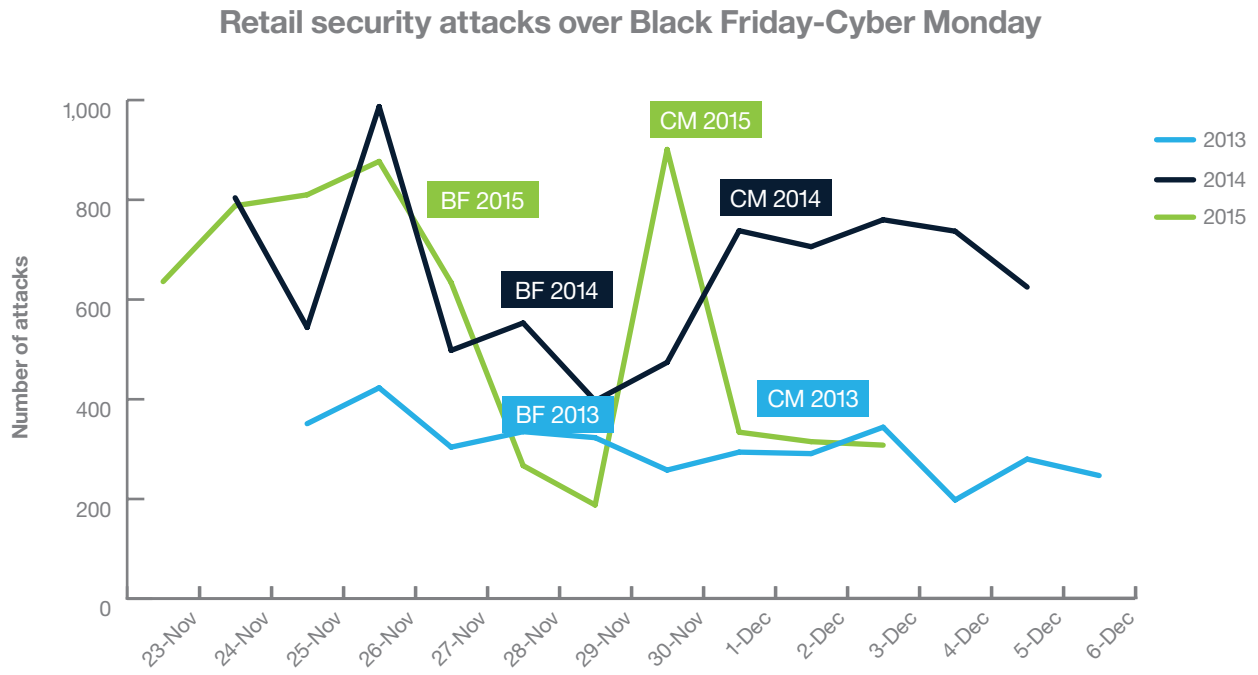
Source: IBM Managed Security Services data.

Figure 4. Security attacks, all industries, 2013–2015 (Black Friday through Cyber Monday).

Contents

Serious compromises and attacks do of course occur during the holidays. The lower-than-anticipated number of daily security attacks during this time might be the result of attackers doing their dirty work earlier in the year so they can reap the benefits during the holiday shopping frenzy. Often, attackers infiltrate systems and then spend months stealthily collecting data before any announcement is made or the organization becomes aware of the compromise.

It's also possible that user education has positively impacted this security trend. There are so many warnings during the holiday season that users may actually be more wary and are hesitating before they click on the dancing Santa in the holiday e-card that installs malware or the flashing "Discount" image that leads them to a malicious site. The extra seasonal vigilance may also be why there are fewer attack attempts. Why attack when everyone is watching?



Source: IBM Managed Security Services data.

Figure 5. Security attacks, retail, 2013–2015 (Black Friday through Cyber Monday).

Contents

Addressing fraud: PIN vs signature or physical vs virtual?

In October 2015, the shift of credit card fraud liability from card issuers to merchants who have not replaced or upgraded their card processing systems to use EMV technology took effect in the United States. Widely used across Europe and around the world for many years, chip-and-PIN-based cards using EMV generate a unique code every time they are used. They're considered more secure than traditional magnetic-stripe cards in which the code in the strip doesn't change, enabling attackers to compromise the information and make counterfeit physical copies. Currently, all chip cards also come with a magnetic stripe in case chip readers aren't available.

The debate then turns to which is more secure: chip-and-PIN cards or chip-and-signature cards. From a security perspective, opponents of chip-and-PIN-based cards argue that attackers can steal the PIN by reading the magnetic stripe data and using the card to withdraw cash from ATMs. Once merchants are fully compliant and their terminals are chip-enabled, the idea is that the magnetic stripe will be removed from cards. Until then, many view the chip-and-signature method as a more security-sound approach than the chip-and-PIN method—but opponents of that viewpoint argue that anyone can steal a physical chip-and-signature card and just scribble the victim's signature at checkout. With a stolen chip-and-PIN-only card, the thief still needs to obtain the PIN somehow.

The challenge is that technology often advances faster than it can be implemented. Take for instance new versions of operating systems or web browsers. Many consumers continue to use older versions of these products long after the vendors have stopped supporting them. So when it comes to the relative merits of chip-and-PIN versus chip-and-signature cards, are we focusing on two forms of payment that will soon be obsolete? Are physical cards almost things of the past, and shouldn't we be focusing our efforts on future forms of payment?

In all likelihood, perhaps sooner than later, payments are going to move into fully virtual modes and bring a whole new set of security challenges, including those posed by slow adoption. It's not too far-fetched to imagine that physical cards may slowly cease to exist and we'll only be able to buy an item by using our Wallet app and touching our phones to the store's POS or using the retailer's browser plug-in online. Physical cards may eventually go the way of the typewriter or record player and once again, credit card vendors may have to overhaul their POS systems.

Contents

Recommendations

Protect retail and POS systems

Malware is the number one attack vector targeting the retail industry. Organizations should be particularly concerned with securing their endpoint sales mechanisms against this threat. At a minimum, implementation of the following best practices is extremely important.

Update POS software: Ensure that POS applications are using the latest software updates and patches. POS systems, like computers, are vulnerable to malware attacks when required updates aren't downloaded and installed on a timely basis.

Use endpoint protection: Endpoint protection enforces continuous security compliance throughout your organization for all POS endpoints. An intelligent agent on the endpoint assesses and remediates issues in real time.

Restrict access to the Internet: Restrict access to POS system computers or terminals to prevent users from accidentally exposing the POS system to security threats on the Internet. POS systems should only be used online to conduct POS-related activities, not for general Internet use.

Disallow remote access or use two-factor authentication: Remote access allows a user to log into a system as an authorized user without being physically present. Cyber criminals can exploit remote access configurations on POS systems to gain access to networks. To prevent unauthorized access, retailers must disallow remote access to the POS network at all times, or use two-factor authentication for providing remote network access as specified by the Payment Card Industry Data Security Standard (PCI DSS) Requirement 8.3.[16]

Segment POS networks: Segmenting the POS network from user traffic creates an extra layer attackers have to bypass in order to compromise the POS environment. Some companies choose to have one or two computers whose only role is to connect to POS machines. These machines are locked down to certain users and have a whitelist of Internet websites they can contact. Guidance provided by the PCI DSS Requirement 1.2.3 states "Firewalls must be installed between all wireless networks and the CDE [cardholder data environment], regardless of the purpose of the environment to which the wireless network is connected."[17]

Contents

Physically protect POS systems: USB ports should be disabled, card readers should only be placed in secure locations and bolted to counters, and cameras should monitor all activity surrounding these devices. Per PCI DSS Requirement 12.3.3, "Malicious individuals may breach physical security and place their own devices on the network as a 'back door.' Personnel may also bypass procedures and install devices. An accurate inventory with proper device labeling allows for quick identification of non-approved installations."[18] These devices should be continuously monitored via a security information and event management (SIEM) service that can normalize and correlate the data to distinguish real threats from false positives and incorporate threat intelligence to help prioritize security incidents.

Use strong passwords: POS systems are often set up with the default passwords for simplicity. Unfortunately, the default passwords can be easily obtained online by cyber criminals. We strongly recommend that business owners change passwords to their POS systems on a regular basis, using unique account names and complex passwords.

Have a holiday game plan

It's never too soon to work on your game plan for the coming year's holiday shopping season. Although historically, attacks have not spiked during Black Friday/Cyber Monday, organizations must not become lax in their protection strategies during this time. Sometimes it only takes one sophisticated targeted attack to cause substantial financial loss and damage to an organization's brand.

Some things can be done to prepare for cyber attacks before and during the holiday season:

Keep patching: Don't ignore patches during the holidays, and be sure you patch all systems dealing with financial data appropriately. Criminals have a lot to gain if they're successful, and patching can keep them away from the new vulnerabilities they want to exploit.

User education: Users have become wary of holiday-themed phishing techniques, and this appears to have had some success in thwarting attack attempts. Consider implementing a phishing awareness campaign a few weeks before the holiday season to test users' ability to identify phishing attacks. Also arm employees with the skills they need to identify suspicious activity both on the phone and in the store.

Contents

Prepare holiday staff: The employees left to hold down the fort don't have time to figure out the appropriate escalation path during a crisis. Make sure your incident response plans are up to date.

Encourage smart shopping: Warn your consumers of the potential for a lurker using a mobile phone to record their debit card PINs at checkout.

Monitor for false brand advertisements: Work with law enforcement to get the fraudulent brand advertisements removed or alert customers to active scams using your brand name.

Reduce fraud in card present transactions

Credit card fraud is a possibility regardless if chip-and-PIN cards or chip-and-signature cards are used. While many of the recommendations above help to reduce fraud, there are additional steps that both fraud and risk managers as well as the consumer can take to mitigate this risk.

Retailers:

Consider contactless POS systems: These leverage near-field communication (NFC) and allow consumers to use their chip-and-PIN credit cards without the need for physical swiping or reading—reducing the risk of attackers skimming the data.

Consider point-to-point encryption (P2PE): As noted by PCI Security Standards Council guidelines, P2PE encrypts card data at the point of interaction and does not decrypt this data "until the data reaches the solution provider's secure decryption environment."[19]

Consumers:

There are many best practices that consumers may follow to protect against credit card fraud. The U.S. Federal Trade Commission (FTC) lists several on their site[20]; below are a few key practices.

Report a lost or stolen card promptly and check statements regularly for any fraudulent purchases.

Record all of your account numbers, their expiration dates and the phone numbers and store in a secure place.

Refrain from lending your cards or leaving your cards, receipts or statements around your home or office. Shred these items when no longer needed.

Contents

Protect your enterprise while reducing cost and complexity

From infrastructure, data and application protection to cloud and managed security services, IBM Security Services has the expertise to help safeguard your company's critical assets. We protect some of the most sophisticated networks in the world and employ some of the best minds in the business.

IBM offers services to help you optimize your security program, stop advanced threats, protect data and safeguard cloud and mobile. IBM Security Strategy Risk and Compliance Services can help you evaluate your existing security practices—including payment card industry security, identity and IT regulatory compliance needs and gaps—against your business objectives. IBM Cybersecurity Assessment and Response Services are designed to help you prepare for and more rapidly respond to an ever-growing variety of security threats. With IBM Managed Security Services, you can take advantage of industry-leading tools, security intelligence and expertise that will help you improve your security posture—often at a fraction of the cost of in-house security resources.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 20 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Retailers can take steps to protect POS systems and help reduce credit card fraud.

Contents

About the author

Michelle Alvarez, a Threat Researcher and Editor for IBM Managed Security Services, brings more than 10 years of industry experience to her role. Michelle is responsible for researching and analyzing security trends and developing and editing security and threat mitigation thought leadership papers. She joined IBM through the Internet Security Services (ISS) acquisition in 2006. At ISS she served as an analyst and contributed to the development of the X-Force Database, one of the world's most comprehensive threats and vulnerabilities database. For many years, Michelle played an important operational role within the Information Technology-Information Sharing and Analysis Center (IT-ISAC), a non-profit, limited liability corporation formed by members within the information technology sector. She is a regular contributor to the IBM-sponsored security blog, SecurityIntelligence.com, and has her Masters degree in Information Technology.

For more information

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit:

ibm.com/security
For more information on security services, visit:
ibm.com/services/security

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Contents

[1] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEL03050USEN&attachment=SEL03050USEN.PDF

[2] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF

[3] http://www-03.ibm.com/security/xforce/xfisi/

[4] http://www.cnbc.com/2015/11/17/reuters-america-fraud-rates-on-online-transactions-seen-up-during-holidays--study.html

[5] https://en.wikipedia.org/wiki/EMV

[6] http://www-03.ibm.com/security/xforce/xfisi/

[7] http://www-03.ibm.com/security/xforce/xfisi/

[8] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype=PM&htmlfid=SEL03043USEN&attachment=SEL03043USEN.PDF

[9] http://www-03.ibm.com/security/xforce/xfisi/

[10] http://www-03.ibm.com/security/xforce/xfisi/

[11] https://securityintelligence.com/shifu-masterful-new-banking-trojan-is-attacking-14-japanese-banks/

[12] https://securityintelligence.com/dyre-wolf/

[13] http://www-03.ibm.com/security/xforce/xfisi/

[14] http://www-03.ibm.com/security/xforce/xfisi/

[15] http://www.theregister.co.uk/2015/08/08/carphone_warehouse_data_breach/

[16] https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

[17] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

[18] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

[19] https://www.pcisecuritystandards.org/documents/P2PE_v1_1_FAQs_Aug2012.pdf

[20] http://www.consumer.ftc.gov/articles/0216-protecting-against-credit-card-fraud#What

Contents

IBM Security

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
December 2015

IBM

SEL03072-USEN-01